Summary on
"This PIN Can Be Easily Guessed:
Analyzing the Security of Smartphone Unlock PINs"

Lohitanvita Rompicharla

RUID: 211009876

Department of Electrical and Computer Engineering

Objective

As we know digitalization of technology has increased now-a-days, whether it may be bank transactions, bill payments, entertainment, also usage of smartphones for fulfilling these purposes on a click are raising due to its supportive interface and secured digital PINs, biometric systems for unlocking. This also alerts us to be cautious with our unlocking method of smartphones to secure the crucial data in it. There are many known situations when the smartphone unlocking Personal Identification Numbers (PINs) have been compromised and data leakage occurred. The current paper “This PIN Can Be Easily Guessed” is based on the stated issue of securing the PIN from getting compromised. It is the first comprehensive study conducted on smartphone PIN safety by collecting 4- and 6-digit PINs from 1220 participants and comparing them with a dataset of blacklists of both android and iOS users. By means of an analysis from questionnaire and comparison with throttle attackers’ model of guessing the PINs, the authors have suggested that a blacklist of about 10% of the PIN space can provide a balance between usability and security.

Introduction

This research paper ‘This PIN Can Be Easily Guessed’ is based on previous works’ such as ‘Chip-and-PIN’, ‘Understanding Human-Chosen PIN’, ‘Quantifying the Security of Graphical Passwords’ that form the basis for this paper by providing the necessary dataset and analysis. For this research, the authors have conducted an experiment by recruiting 1220 participants who in return provided a dataset of selected 4- or 6-digit PINs used for unlocking the smartphone. This list of PINs is then analyzed in a throttled setting and reports that the benefit of 6-digit PINs is no way better than the 4-digit PINs. An unthrottled attacker can guess offline, indefinitely, until all the secrets are correctly guessed, unlike a throttled attacker who has a limited number of guesses, which matches the reality of attacks. Throttled attacker model is chosen to inspect the different blacklisting approaches that influence the PIN selection process for both usability and security. Then feedback is obtained through a questionnaire on the basis of memorability, security, ease-of-use of PIN-based authentication from the participants to determine a blacklist that secures the PIN selection. In throttled attacker model, considering an un-targeted attacker who does not have additional information about the victim being attacked, open-source PIN datasets Amitay-4-digit and RockYou-6-digit are collected to guess the PIN since the only way he can guess the PIN is in decreasing probability order. In case of a targeted attacker with the knowledge of blacklist, he can improve guessing by eliminating blacklisted PINs, therefore a list of blacklisted PINs are collected from LinkedIn password leakage, Rock You leak, ‘easily guessed’ (Apple used blacklist), also a Raspberry Pi based automated module is devised for obtaining 10000 4-digit PINs and 1 million 6-digit PINs from iPhone that are named as iOS-4 and iOS-6 blacklists to perform guessing work. Also, rate limits of Android and iOS mobile operating systems are tabulated. This whole information is then used for determining strength estimations and comparisons by guiding the developers to choose an approximately sized PIN blacklist that can have a noticeable impact.

Working

For achieving qualitative and quantitative feedback on users’ perception of security, memorability, and ease-of-use a user study with 851 4-digit and 369 6-digit PINs was conducted on Amazon Mechanical Turk (MTurk) with 1220 participants. Nine different treatments (six 4-digit and three 6-digit PINs treatments) were applied between the PIN selection criteria that are categorized as Control Treatments, Blacklist Treatments in which the users can select any PIN in their ‘first attempt’ without being subjected to blacklist. The next time when they select a new PIN, the blacklist is implemented, either enforcing or non-enforcing blacklist. In enforcing blacklist, the user is not allowed to continue until a non-blacklisted PIN is selected, but in non-enforcing blacklist, the user is given an option to either continue with the weak PIN

or can change to more secured once. Placebo backlist, iOS backlist and Data-Drive Blacklists containing user-entered first PINs,‘easy guessed’ blacklist of apple phone and two 4-digit blacklists that are significantly (10x) smaller (27 PINs) and (10x) larger (2740 PINs) than the iOS blacklist referred as DD-4-digit-27 and DD-4-digit-2740., respectively, are used for comparison of the recently selected PINs. This selection strategies include one small (27 4-digit PINs), one large (2740 4-digit PINs), and two blacklists (274 4-digit PINs and 2910 6-digit PINs) in use today on iOS devices. Based on this experiment a user is then questioned about the blacklisting event, PIN selection process, and recalling the previous PINs they have experienced to report the required metrics. Secondly, for achieving security and usability, a throttled attacker model is designed to identify the attacker's process of guessing the PIN and using the data for improving the security. While performing the user study, data about usage of mobile unlock authentication scheme was also collected that informs whether fingerprint, face recognition, PIN, pattern, alphanumeric is highly used. The results show that PINs are the most highly used unlock schemes, therefore guessing the PIN is the primary solution for securing information in the phone. In throttled attack model, an online guessing (targeted attacker) and offline guessing (un-targeted attacker) of PIN selection are made. For targeted attacker assuming that he always guesses correctly, an entropy-based strength metric is utilized. The respective, min-entropy H and guessing entropy G is calculated for First-4, Amit-4, Rock-4, Rock-6 where H lower bound is dependent on most common PIN (1234,123456) and tabulated for comparison. Now taking an un-targeted attacker case, we apply the Guess Number-Driven Strength Estimates, i.e., guessing with decreasing probability order with respect to the rate limit of iOS and Android. A total of 100 guesses are performed and graphed for all four datasets and the following result is obtained: for the first 10 guesses 4.6 % 4-digit and 6.5 % 6-digit are guessed, for 30 guesses 7.6 % 4-digit and 8.9 % 6-digit are guesses, lastly, for 100 guesses 16.2 % of the 4-digit and 13.3 % of 6-digit PINs were guessed. This implies a 6-digits PIN does not offer any security advantage over a 4-digit PIN in a throttled guessing attacker.

Conclusion

The research on “This PIN Can Be Easily Guessed” was conducted in a very efficient way by considering all possible situations from iOS, Android datasets, blacklists from different sources to considering human thoughts and opinions on the process. Based on its principles and working we can conclude that for throttled attack scenario, the solution obtained by just increasing PIN from 4- to 6-digit does not increase the complexity. From the rate limits of iOS and Android, we know that iOS supports only 10 guesses whereas Android supports more than 100 guesses with a wait time of 10 hours, in such a context PIN space would need to contain 10 % of the blacklist.

Future Scope

Though the current experiment achieved its planned goal, it still has a little scope of improvement in few below mentioned major scenarios: i) experiment was performed with a certain age group of people situated in the US only, so further it can be extended to age-diverse and location-diverse population, ii) warning message limitations while enforcing blacklist can be furthermore analyzed for better quality, iii) reason behind the inefficiency of 6-digit PIN selection need to figured out with different set of information and setup.